USER GUIDE

KASPERSKY ANTI-VIRUS 2009

Dear User of Kaspersky Anti-Virus 2009!

Thank you for choosing our product. We hope that this documentation helps you in your work and provides answers regarding this software product.

Warning! This document is the property of Kaspersky Lab: all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts thereof will result in civil, administrative or criminal liability in accordance with the laws of the Russian Federation. Any type of reproduction or distribution of any materials, including in translated form, is allowed only with the written permission of Kaspersky Lab. This document and the graphic images it contains can be used exclusively for information, non-commercial or personal purposes.

This document may be amended without prior notification. For the latest version, refer to Kaspersky Lab's website at http://www.kaspersky.com/docs. Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document for which the rights are held by third parties, or for the potential damages associated with using such documents.

This document includes registered and non-registered trademarks. All trademarks are the property of their owners.

© Kaspersky Lab, 1996-2008

+7 (495) 645-7939,
Tel., fax: +7 (495) 797-8700,
+7 (495) 956-7000

http://www.kaspersky.com/
http://support.kaspersky.com/

Revision date: 13.11.2008

TABLE OF CONTENTS

INTRODUCTION 5
Obtaining information about the application 5
Sources of information to research on your own 5
Contacting the Sales Department 6
Contacting the Technical Support service 6
Discussing Kaspersky Lab applications on the web forum 8
What's new in Kaspersky Anti-Virus 2009 8
Overview of application protection 9
Wizards and tools 10
Support features 11
Heuristic analysis 12
Hardware and software system requirements 13
THREATS TO COMPUTER SECURITY 15
Threat applications 15
Malicious programs 16
Viruses and worms 16
Trojans 20
Malicious utilities 26
Potentially unwanted programs 29
Adware 30
Pornware 30
Other Riskware programs 31
Methods of detecting infected, suspicious and potentially dangerous objects by the application 35
INSTALLING THE APPLICATION 36
Step 1. Searching for a newer version of the application 37
Step 2. Verifying the system satisfies the installation requirements 38
Step 3. Wizard's greeting window 38
Step 4. Viewing the License Agreement 39
Step 5. Selecting the installation type 39
Step 6. Selecting the installation folder 40

Step 7. Selecting application components to be installed 40
Step 8. Searching for other anti-virus software 41
Step 9. Final preparation for the installation 42
Step 10. Completing the installation 43
APPLICATION INTERFACE 44
Notification area icon 44
Shortcut menu 45
Main application window 47
Notifications 50
Application settings window 50
GETTING STARTED 52
Updating the application 53
Security analysis 54
Scanning computer for viruses 54
Managing license 55
Subscription for the automatic license renewal 56
Participating in the Kaspersky Security Network 59
Security management 60
Pausing protection 62
VALIDATING APPLICATION SETTINGS 64
Test the EICAR “virus” and its modifications 64
Testing the HTTP traffic protection 68
Testing the SMTP traffic protection 68
Validating File Anti-Virus settings 69
Validating virus scan task settings 70
KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT 71
KASPERSKY LAB 77
CRYPTOEX LLC 80
MOZILLA FOUNDATION 81
LICENSE AGREEMENT 82

INTRODUCTION

IN THIS SECTION:

Obtaining information about the application 5

What's new in Kaspersky Anti-Virus 2009 8

Overview of application protection 9

Hardware and software system requirements 13

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have any questions regarding purchasing, installing or using the application, answers are readily available.

Kaspersky Lab has many sources of information, from which you can select the most convenient, depending on the urgency and importance of your question.

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the Help system.

The Help system contains information on managing the computer protection: how to view the protection status, scan various areas of the computer and perform other tasks.

To open Help, click the **Help** link in the main application window, or press **<F1>**.

CONTACTING THE SALES DEPARTMENT

If you have questions regarding selecting or purchasing the application or extending the period of its use, you can phone Sales Department specialists in our Central Office in Moscow at:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

The service is provided in Russian or English.

You can send your questions to the Sales Department to the e-mail address sales@kaspersky.com.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you already purchased the application you can obtain information about it from the Technical Support service by phone or via the Internet.

The Technical Support service specialists will answer your questions about regarding the installation and the use of the application and if your computer has been infected, will help you eliminate the consequences of the activities of malware.

An e-mail request to the Technical Support service (for registered users only)

You can ask your question to the Technical Support Service specialists by filling out a Helpdesk web form (http://support.kaspersky.com/helpdesk.html).

You can write your question in Russian, English, German, French or Spanish.

To send an e-mail message with your question, you must enter the **client number** and **password** which you obtained during registration at the Technical Support service website.

Note

If you are not yet a registered user of Kaspersky Lab's applications, you can fill out a registration form at https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/. During registration you will have to supply the activation code or key file name.

The Technical Support service will respond to your request in your **Personal Cabinet** at https://support.kaspersky.com/en/PersonalCabinet, and to the e-mail address you specified in your request.

In the request web form, describe the problem you encountered in as much detail as possible. Specify the following information in the mandatory fields:

- **Prompt type**. Questions most frequently asked by users are grouped into special topics, for example "Product installation/removal problem" or "Virus scan/removal problem". If there is no appropriate topic for your question, select the topic "General Question".

- **Application name and version number**.

- **Prompt text**. Describe the problem you encountered in as much detail as possible.

- **Client number and password**. Enter the client number and password which you received during registration at the Technical Support service website.

- **E-mail address**. The Technical Support service will send their answer to this e-mail address.

Technical support by phone

If you have a problem which requires urgent help, you can call your nearest Technical Support office. You will need to supply identifying information (http://support.kaspersky.com/support/details) when you apply to Russian (http://support.kaspersky.com/support/support_local) or international (http://support.kaspersky.com/support/international) Technical Support. This will help our specialists to process your request as soon as possible.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other Kaspersky software users in our web forum, located at http://forum.kaspersky.com/.

In this forum you can view existing topics, leave your replies, create new topics and use the search engine.

WHAT'S NEW IN KASPERSKY ANTI-VIRUS 2009

Kaspersky Anti-Virus 2009 (also referred to as “Kaspersky Anti-Virus” or “the application”) uses a totally new approach to data security, based on restricting each program’s rights to access system resources. This approach helps prevent unwanted actions by suspicious and hazardous programs. The application's ability to protect each user's confidential data has also been considerably enhanced. The application now includes wizards and tools which substantially simplify specific computer protection tasks.

Let's review the new features of Kaspersky Anti-Virus 2009:

New Protection Features:

- Scanning the operating system and installed software to detect and eliminate vulnerabilities, maintains a high system security level and prevents hazardous programs penetrating your system.

- The new Security Analyzer and Browser Configuration wizards facilitate scanning for, and elimination of, security threats and vulnerabilities in installed programs, and in the configuration of the operating system and browser.

- Kaspersky Lab now reacts more quickly to new threats through the use of the Kaspersky Security Network, which gathers data about the infection of users' computers and sends it to Kaspersky Lab's servers.

- The new System Restore wizard helps repair damage to your system arising from malware attacks.

New protection features for internet use:

- Protection against internet intruders has been improved by including the addresses of phishing sites in the application's databases.

- Secure use of instant messaging is provided by a tool which scans ICQ and MSN traffic.

The application's new interface features:

- The application's new interface reflects the comprehensive approach to information protection.

- The high information capacity of dialog boxes helps the user make quick decisions.

- The functionality for recording statistics and making reports has been extended. Filters can be used to select data from reports, a powerful and flexible tool which is irreplaceable for professionals.

OVERVIEW OF APPLICATION PROTECTION

Kaspersky Anti-Virus protects your computer against known and unknown threats, and against unwanted data. Each type of threat is processed by a separate application component. This makes setup flexible, with easy configuration options for all components, which can be tailored to the needs of a specific user or of the business as a whole.

Kaspersky Anti-Virus includes the following protective features:

- Monitors system activities by user applications, preventing any dangerous actions by applications.

- Protection components provides real-time protection of all data transfer and input paths through your computer.

- Online Security provides protection against phishing attacks.

- Virus scan tasks are used to scan individual files, folders, drives, specified areas, or the entire computer for viruses. Scan tasks can also be configured to detect vulnerabilities in installed user applications.

- The updating component ensures the up to date status of both the application's modules and the databases used to detect malicious programs, hacker attacks and spam messages.

- Wizards and tools facilitate the execution of tasks occurring during Kaspersky Anti-Virus's operation.

- Support features, which provide information and assistance for working with the application and expanding its capabilities.

WIZARDS AND TOOLS

Ensuring computer security is a complex task which requires knowledge of the operating system's features and the methods used to exploit its weaknesses. Additionally, the volume and diversity of information about system security make its analysis and processing difficult.

To help solve specific tasks in providing computer security, the Kaspersky Anti-Virus package includes a set of wizards and tools.

- Security Analyzer wizard performs computer diagnostics, searching for vulnerabilities in the operating system and in user programs installed on the computer.

- Browser Configuration Wizard analyses the Microsoft Internet Explorer browser settings, evaluating them primarily from a security point of view.

- System Restore wizard eliminates any traces of malware attacks on the system.

- Rescue Disk wizard restores system functionality after a virus attack has damaged the operating system's files and made it impossible to restart the computer.

SUPPORT FEATURES

The application includes a number of support features which are designed to keep the application up-to-date, to expand the application's capabilities, and to assist you in using it.

Kaspersky Security Network

Kaspersky Security Network is a system which automatically transfers reports about detected and potential threats to Kaspersky Lab's central database. This database allows Kaspersky Lab to respond more quickly to the most widespread threats, and to notify users about virus outbreaks.

License

When you purchase Kaspersky Anti-Virus, you enter into a licensing agreement with Kaspersky Lab which governs the use of the application, your access to application database updates, and Technical Support for a specified period of time. The term of use and other information necessary for the application's full functionality are included in the license key file.

Using the **License** function you can obtain detailed information about your current license, purchase a new license or renew your current one.

Support

All registered Kaspersky Anti-Virus users can take advantage of our technical support service. To see information about how to receive technical support, use the **Support** function.

By following the links you can access the Kaspersky Lab product users' forum, send an error report to Technical Support, or give application feedback by completing a special online form.

You also have access to the online Technical Support and Personal User Cabinet Services. Our personnel are always happy to provide you with telephone support about the application.

HEURISTIC ANALYSIS

Heuristics are used in some real-time protection components, such as File Anti-Virus, Mail Anti-Virus, and Web Anti-Virus, and in virus scans.

Scanning objects using the signature method, which uses a database containing descriptions of all known threats, gives a definite answer as to whether a scanned object is malicious, and what danger it presents. The heuristic method, unlike the signature method, aims to detect the typical behavior of objects rather than their static content, but cannot provide the same degree of certainty in its conclusions.

The advantage of heuristic analysis is that it detects malware that is not registered in the database, so that you do not have to update the database before scanning. Because of this, new threats are detected before virus analysts have encountered them.

However, there are methods for circumventing heuristics. One such defensive measure is to freeze the activity of malicious code as soon as the object detects the heuristic scan.

Note
Using a combination of scanning methods ensures greater security.

When scanning an object, the heuristic analyzer emulates the object's execution in a secure virtual environment provided by the application. If suspicious activity is discovered as the object executes, it will be deemed malicious and will not be allowed to run on the host, and a message will be displayed requesting further instructions from the user:

- Quarantine the object, allowing the new threat to be scanned and processed later using updated databases.
- Delete the object.
- Skip (if you are positive that the object cannot be malicious).

To use heuristic methods, check the box **Use heuristic analyzer** and move the scan detail slider to one of these positions: Shallow, Medium, or Detailed. The level of detail of the scan provides a balance between the thoroughness, and hence the quality, of the scan for new threats, and the load on operating system

resources and the scan's duration. The higher you set the heuristics level, the more system resources the scan will require, and the longer it will take.

Warning!

New threats detected using heuristic analysis are quickly analyzed by Kaspersky Lab, and methods for disinfecting them are added to the hourly database updates.

If you regularly update your databases, you will be maintaining the optimal level of protection for your computer.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

To allow the computer to function normally, the computer must meet these minimum requirements:

General requirements:

- 75 MB free hard drive space.
- CD-ROM (for installation of the application from the installation CD).
- A mouse.
- Microsoft Internet Explorer 5.5 or higher (for updating the application's databases and software modules via the Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 or above), Microsoft Windows XP Professional (SP2 or above), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHz processor or higher (or a compatible equivalent).
- 256 MB RAM.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).

- 512 MB RAM.

THREATS TO COMPUTER SECURITY

Computer security can be compromised by threat applications, spam, phishing, hacker attacks, ad-ware and banners. The main source of these threats is the internet.

IN THIS SECTION:

Threat applications 15

THREAT APPLICATIONS

Kaspersky Anti-Virus can detect thousands of malware programs that may reside on your computer. Some of these programs represent a constant threat to your computer, while others are only dangerous in certain conditions. After the application detects a malware application, it classifies it and assigns it a danger level (high or medium).

Kaspersky Lab's virus analysts distinguish two main categories of threat application: *malware programs* and *potentially unwanted programs.*

Malware programs (Malware) (see page 16) are created to damage the computer and its user: for example, to steal, block, modify or erase information, or to disrupt the operation of a computer or a computer network.

Potentially unwanted programs (PUPs) (see page 29), unlike malware programs, are not intended solely to inflict damage but can assist in penetrating a computer's security system.

The Virus Encyclopedia (http://www.viruslist.com/en/viruses/encyclopedia) contains a detailed description of these programs.

MALICIOUS PROGRAMS

Malicious programs (“malware”) are created specifically to inflict harm on computers and their users: to steal, block, modify or erase information, or to disrupt the operation of computers or computer networks.

Malware programs are divided into three subcategories: *viruses and worms, Trojans programs* and *malware utilities*.

Viruses and worms (Viruses_and_Worms) (see page 16) can create copies of themselves, which in turn spread and reproduce again. Some of them run without the user's knowledge or participation, others require actions on the user's part to be run. These programs perform their malicious actions when executed.

Trojan programs (Trojan_programs) (see page 20) do not create copies of themselves, unlike worms and viruses. They infect a computer, for example, via e-mail or via a web browser when the user visits an “infected” website. They must be launched by the user, and perform their malicious actions when run.

Malware utilities (Malicious_tools) (see page 26) are created specifically to inflict damage. However, unlike other malware programs, they do not perform malicious actions as they are run and can be safely stored and run on the user's computer. They have functions which hackers use to create viruses, worms and Trojan programs, to arrange network attacks on remote servers, hack computers or perform other malicious actions.

VIRUSES AND WORMS

Subcategory: viruses and worms (Viruses_and_Worms)

Severity level: high

Classic viruses and worms perform unauthorized actions on the infected computer, including replicating and spreading themselves.

Classic virus

After a classic virus infiltrates the system, it infects a file, activates itself, performs its malicious action, and adds copies of itself to other files.

Classic viruses reproduce only within the local resources of the infected computer, but cannot independently penetrate other computers. Distribution to other computers can occur only if the virus adds itself to a file stored in a shared folder or on a CD, or if the user forwards an e-mail message with an infected attachment.

The code of a classic virus is usually specialized to penetrate a particular area of a computer, operating system or application. Based on the environment, there is a distinction between *file, boot, script and macro viruses.*

Viruses can infect files using various methods. *Overwriting* viruses write their own code to replace the code of the infected file, destroying the original contents of the file. The infected file stops working and cannot be disinfected. *Parasitic viruses* modify files leaving them fully or partially operating. *Companion viruses* do not modify files but duplicate them, so that when the infected file is opened, its duplicate, that is the virus, will run instead. Other types of viruses include *link viruses*, OBJ viruses that *infect object modules*, LIB viruses that *infect compiler libraries*, and viruses that *infect original text of programs*.

Worm

After it penetrates the system, a network worm, similarly to the classic virus, becomes activated and performs its malicious action. The network worm is named for its ability to tunnel secretly from one computer to another, to propagate itself through various information channels.

Worms are categorized by their primary method of proliferation, which are listed in the table below:

Table 1. Worms categorized by the method of proliferation

TYPE	NAME	DESCRIPTION
Email-Worm	E-mail worms	E-mail worms infect computers via e-mail. The infected message has an attached file containing either a copy of a worm, or a link to a worm file uploaded to a website. The website is usually either one that has been hacked, or is the hacker's own site. When the attachment is opened the worm is activated; alternatively, when you click the link, download and open the file, the worm will become active. After this the worm will continue reproducing by finding other e-mail addresses and sending infected messages to them.
IM-Worm	IM worms	These worms propagate through IM (instant messaging) clients, such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager and Skype. Usually these worms use contact lists to send messages containing a link to a worm file on a website. When a user downloads and opens the file, the worm is activated.
IRC-Worms	IRC worms	Worms of this type get into computers through Internet Relay channels, which are used to communicate with other people via the internet in real time. These worms publish on the internet chat channel, either a copy of the worm file, or a link to the file. When a user downloads and opens the file, the worm will be activated.

TYPE	NAME	DESCRIPTION
Net-Worms	Network worms (worms residing in computer networks)	These worms are distributed via computer networks. Unlike other types of worms, network worms propagate without the user's participation. They search the local area network for computers which host programs containing vulnerabilities. They do this by broadcasting a special network packet (exploit) containing its code or a part of its code to each computer. If there is a vulnerable computer in the network, it will be infiltrated by the packet. Once the worm fully penetrates the computer, it becomes active.
P2P-Worm	File exchange worms	File exchange worms propagate through file-exchange peer-to-peer networks, such as Kazaa, Grokster, EDonkey, FastTrack or Gnutella. To use a file exchange network, the worm copies itself into the file-exchange folder which is usually located on the user's computer. The file-exchange network displays information about the file and the user can “find” the infected file in the network, like any other file, download it and open it. More complex worms imitate the network protocols of a specific file exchange network: they provide positive responses to search requests and offer copies of themselves for downloading.

TYPE	NAME	DESCRIPTION
Worm	Other worms	Other network worms include: • Worms that distribute their copies via network resources. Using the operating system's functionality, they go through available network folders, connect to computers in the global network and attempt to open their drives for full access. Unlike computer network worms, the user has to open a file containing a copy of the worm to activate it. • Worms that use other propagation methods not listed here: for example, worms propagating via mobile phones.

TROJANS

Subcategory: Trojans (Trojan_programs)

Severity level: high

Unlike worms and viruses, Trojan programs do not create copies of themselves. They infect a computer, for example, via an infected e-mail attachment, or through a web browser when the user visits an “infected” website. Trojan programs must be launched by the user, and start performing their malicious actions as they run.

Trojan programs can perform a range of malicious actions. The major functions of Trojans are blocking, modifying and erasing data, and disrupting the operation of computers or computer networks. Additionally, Trojan programs can receive and send files, run them, display messages, access web pages, download and install programs and restart the infected computer.

Intruders often use “sets” consisting of complementary Trojan programs.

The different types of Trojan programs and their behavior are described in the table below.

Table 2. Types of trojan programs categorized by behavior on the infected computer

TYPE	NAME	DESCRIPTION
Trojan-ArcBomb	Trojan programs - archive bombs	Archives which when unpacked increase to a size that disrupts the computer's operation. When you attempt to unpack the archive, the computer may start working slowly or "freeze", and the disk may be filled with "empty" data. "Archive bombs" are especially dangerous for file and mail servers. If an automatic incoming information processing system is used on the server, such an "archive bomb" can stop the server.
Backdoor	Remote administration Trojan programs	These programs are considered the most dangerous among Trojan programs; function-wise they are similar to off-the-shelf remote administration programs. These programs install themselves without the user's knowledge, and give the intruder remote management of the computer.
Trojans	Trojans	Trojans include the following malicious programs: • **classic Trojan programs**, which only perform the major functions of Trojan programs: blocking, modifying or erasing data, disrupting the operation of computers or computer networks. They do not have the additional functions characteristic of other types of Trojan programs described in this table; • **"multi-purpose"** Trojan programs, which do have additional functions characteristic of several types of Trojan programs.

TYPE	NAME	DESCRIPTION
Trojan-Ransoms	Trojan programs requiring a ransom	They “take hostage” information on the user's computer, modifying or blocking it or disrupting the computer’s operation so that the user cannot use the data. Then the intruder demands a ransom from the user, in exchange for a promise to send the program that will restore the computer's operability.
Trojan-Clickers	Trojan-Clickers	These programs access web pages from the user's computer: they send a command to the web browser, or replace web addresses stored in the system files. Using these programs the intruders arrange network attacks, or increase the traffic to particular sites to boost revenues from displaying ad banners.
Trojan-Downloaders	Trojan downloader-programs	These programs access the intruder's web page, download other malware programs from it, and install them on the user's computer. They can either store the name of the downloadable malware program filename in their own code, or receive it from the web page they access.

TYPE	NAME	DESCRIPTION
Trojan-Droppers	Trojan program-droppers	These programs save programs containing other Trojan programs on the computer's disk and then install them. Intruders can use Trojans-Droppers in different ways: • to install malware programs without the user's knowledge: Trojans-droppers either do not display any messages, or display false messages, for example, notifying about an error in an archive or about using the wrong version of the operating system; • to protect another known malware program from being detected: not every anti-virus program can detect a malware program located inside a trojan-dropper.
Trojan-Notifiers	Trojan-notifiers	They notify the intruder that the infected computer is connected; and then transfer information about the computer to the intruder, including: IP address, number of an open port or the e-mail address. They communicate to the intruder using a number of methods including e-mail, FTP, and by accessing the intruder's web page. Trojan-notifiers are often used in sets of complementary Trojan programs. They notify the intruder that other Trojan programs are successfully installed on the user's computer.

TYPE	NAME	DESCRIPTION
Trojan-Proxies	Trojan-Proxies	They allow the intruder to access web pages anonymously using the identity of the user's computer, and are often used to send spam.
Trojan-PSWs	Trojans stealing passwords	Trojans stealing passwords (Password Stealing Ware); they steal users' accounts, for example, software registration information. They find confidential information in system files and in the registry and send it to their developer using methods which include e-mail, FTP, and by accessing the intruder's website. Some of these Trojan programs fall into specific types described in this table, Including Trojan-Bankers, Trojans-IMs and Trojans-GameThieves.
Trojan-Spies	Trojan spy programs	These programs are used for spying on the user: they collect information about the user's actions on the computer: for example, they intercept data entered by the user at the keyboard, make snapshots of the screen and collect lists of active applications. After they receive this information, they transfer it to the intruder using methods including e-mail, FTP, or by accessing the intruder's website.
Trojan-DoS	Trojan programs - network attacks	For a Denial-of-Service (DoS) attack, the Trojan will send numerous requests from the user's computer to a remote server. The server will exhaust its resources processing these requests and will stop functioning. These programs are often used to infect multiple computers to make a combined attack on the server.

TYPE	NAME	DESCRIPTION
Trojan-IMs	Trojan programs stealing personal data of IM client users	These programs steal numbers and passwords of IM client users (instant messaging programs), such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager or Skype. They transfer information to the intruder using methods which include e-mail, FTP, and by accessing the intruder's website.
Rootkits	Rootkits	These programs conceal other malware programs and their activity and, thus, extend the existence of such programs in the system. They hide files, processes in the memory of an infected computer, or registry keys run by the malware programs, or conceal data exchange between applications installed on the user's computer and other computers in the network.
Trojan-SMS	Trojan programs - SMS messages	These programs infect mobile phones and send SMS messages to numbers for which the user of the infected phone is charged.
Trojan-GameThieves	Trojan programs stealing personal data of the users of network games.	These programs steal user account information of network game users; they then transfer this information to the intruder using methods including e-mail, FTP, or by accessing the intruder's website.
Trojan-Bankers	Trojan programs stealing banking account information	These programs steal banking account information or electronic/digital money account information; they transfer data to the intruder using methods including e-mail, FTP, or by accessing the intruder's website.

TYPE	NAME	DESCRIPTION
Trojan-Mailfinders	Trojan programs that collect e-mail addresses	These programs collect e-mail addresses on the computer and transfer them to the intruder using methods including e-mail, FTP, and by accessing the intruder's website. The intruder can use the collected addresses to send spam.

MALICIOUS UTILITIES

Subcategory: malicious utilities (Malicious_tools)

Severity level: medium

These utilities are designed specifically to inflict damage. However, unlike other malware programs, they are tools used primarily to attack other computers, and can be safely stored and run on the user's computer. These programs provide functionality to help create viruses, worms and Trojan programs, to arrange network attacks on remote servers, to hack computers and other malicious actions.

There are many types of malware utilities with different functions, which are described in the table below.

Table 3. Malware utilities grouped by function

TYPE	NAME	DESCRIPTION
Constructor	Constructors	Constructors are used to create new viruses, worms and Trojan programs. Some constructors have a standard Windows interface, allowing the hacker to select the type of the malicious program to be created, the method this program will use to resist debugging, and other similar properties.
DoS	Network attacks	Denial-of-Service (DoS) programs send numerous requests from the user's

TYPE	NAME	DESCRIPTION
		computer to the remote server. The server will then exhaust its resources for processing requests, and will stop functioning.
Exploit	Exploits	An exploit is a set of data, or a piece of program code, which uses an application's vulnerabilities to perform a malicious action on the computer. For example, exploits can write or read files, or access “infected” web pages. Different exploits use the vulnerabilities of different applications or network services. An exploit is transferred via the network to multiple computers in the form of a network packet, searching for computers with vulnerable network services. For example, an exploit contained in a DOC file looks for vulnerabilities of text editors, and when the user opens an infected file, can start performing functions programmed by the intruder. An exploit contained in an e-mail message searches for vulnerabilities in e-mail client programs; it can start performing its malicious action as soon as the user opens an infected message using this program. Exploits are also used to distribute net worms (Net-Worm). Exploit-Nukers are network packets that make computers inoperative.
FileCryptors	File Cryptors	File cryptors encrypt other malicious programs, to hide them from anti-virus applications.

TYPE	NAME	DESCRIPTION
Flooders	Programs used for flooding networks	These programs send a great number of messages via network channels, including, for example, internet relay chat channels. However, this category of malware does not include programs which flood e-mail traffic, or IM and SMS channels, which are separately classified in the table below (Email-Flooder, IM-Flooder and SMS-Flooder).
HackTools	Hacking Tools	Hacking tools are used to hack computers on which they are installed, or to arrange attacks on another computer. Such attacks include: creating new system user accounts without permission, or clearing the system logs to conceal any traces of the new user's presence in the system. They include some sniffers which perform malicious functions, for example, intercepting passwords. Sniffers are programs which allow the examination of network traffic.
not-virus:Hoax	Hoax programs	These programs scare the user with virus-like messages: they "detect" a virus in a clean file, or display a message about disk formatting which will not take place.
Spoofers	Spoofers	These programs send messages and network requests with a fake sender's address. Intruders use spoofers in order, for example, to pretend to be a legitimate sender.
VirTools	They are tools used to create modifications of malware programs	They make it possible to modify other malware programs to hide them from anti-virus applications.

TYPE	NAME	DESCRIPTION
Email-Flooders	Programs for flooding e-mail addresses	These programs send numerous messages to e-mail addresses (flood them). Due to the large flow of messages, users are unable to view incoming messages which are not spam.
IM-Flooders	Programs used for flooding IM programs	These programs send numerous messages to Instant Messaging (IM) client programs, such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager or Skype. Due to the large flow of messages, users are unable to view incoming messages which are not spam.
SMS-Flooders	Programs used for flooding with SMS text messages	These programs send numerous SMS messages to mobile phones.

POTENTIALLY UNWANTED PROGRAMS

Potentially unwanted programs, unlike malware programs, are not intended solely to inflict damage. However they can be used to breach the computer's security.

Potentially unwanted programs include *adware, pornware* and *other potentially unwanted programs*.

Adware programs (see page 30) display advertising information to the user.

Pornware programs (see page 30) display pornographic information to the user.

Other Riskware programs (see page 31) are frequently useful programs used by many computer users. However, if an intruder obtains access to these programs or installs them on the user's computer, the intruder can use them to breach the computer's security.

Potentially unwanted programs are installed using one of the following methods:

- They are installed by the user, individually or together with another program. For example, software developers frequently include adware programs in freeware or shareware programs.

- They are also installed by intruders. For example, they include such programs in packages with other malware programs, using "vulnerabilities" of the web browser, or Trojan downloaders and droppers, when the user visits an "infected" website.

ADWARE

Subcategory: Adware

Severity level: medium

Adware programs display advertising information to the user. They display ad banners in another program's interface, and redirect search queries to advertising websites. Some adware programs collect, and send to their developer, marketing information about the user: for example, which sites they visit, or which search requests they make. Unlike Trojan spies, this information is transferred with the user's permission.

PORNWARE

Subcategory: Pornware

Severity level: medium

Usually, users install these programs themselves, to search for or download pornographic information.

Intruders can also install these programs on the user's computer to display ads for commercial pornographic sites and services to the user, without the user's permission. To be installed, they use vulnerabilities of the operating system or web browser, and are generally distributed by Trojan downloaders and Trojan droppers.

There are three types of pornware programs, as categorized in the table below.

Table 4. Types of pornware programs categorized by their functions

TYPE	NAME	DESCRIPTION
Porn-Dialers	Automatic dialers	These programs contain the phone numbers of pornographic phone services and automatically dial them; unlike Trojan dialers, they notify users about their actions.
Porn-Downloaders	Programs for downloading files from the Internet	These programs download pornographic information to the user's computer; unlike Trojan dialers, they notify users about their actions.
Porn-Tools	Tools	They are used to search for and display pornography; this type include special browser toolbars, and special video players.

OTHER RISKWARE PROGRAMS

Subcategory: other riskware programs

Severity level: medium

Most of these programs are useful programs, in common legitimate use. They include IRC clients, dialers, file downloading management programs, computer system activity monitors, password management utilities, and FTP, HTTP or Telnet servers.

However, if an intruder obtains access to these programs, or installs them on the user's computer, their functionality can be used to breach the computer's security.

The table lists riskware programs, grouped by function.

Table 5. Types of other riskware grouped by function

TYPE	NAME	DESCRIPTION
Client-IRC	Internet chat client programs	Users install these programs to communicate through Internet Relay Channels. Intruders use them to spread malware programs.
Dialers	Automatic dialing programs	These programs can establish “hidden” phone connections via the modem.
Downloaders	Downloaders	These programs can secretly download files from websites.
Monitors	Monitors	These programs monitor the activities of computers on which they are installed, including monitoring the performance of applications, and of data exchange operations with applications on other computers.
PSWTools	Password recovery tools	These programs are used to view and recover forgotten passwords. Intruders use them in exactly the same way when they install them on users' computers.

TYPE	NAME	DESCRIPTION
RemoteAdmin	Remote administration programs	These programs are often used by system administrators; they provide access to a remote computer, to monitor and manage it. Intruders use them in exactly the same way when they install them on users' computers. Remote administration riskware programs are different from Trojan (or Backdoor) remote administration programs. Trojan programs can independently infiltrate the system and install themselves; legitimate programs do not have this functionality.
Server-FTP	FTP servers	These programs perform the functions of FTP servers. Intruders install them on users' computers to obtain remote access via FTP protocol.
Server-Proxy	Proxy servers	These programs perform the functions of proxy servers. Intruders install them on users' computers to send spam using the users' identitues.
Server-Telnet	Telnet servers	These programs perform the functions of Telnet servers. Intruders install them on the users' computers to obtain remote access via the Telnet protocol.
Server-Web	Web servers	These programs perform the functions of web servers. Intruders install them on the users' computers to obtain remote access via the HTTP protocol.

TYPE	NAME	DESCRIPTION
RiskTool	Local computer tools	These tools provide users with additional functionality and are used within the user's computer only. They allow the hacker to hide files, hide the windows of active applications, or to close active processes.
NetTool	Network tools	These tools allow a computer user to remotely manage other computers on the network: for example, to restart them, find open ports, or run programs installed on these computers.
Client-P2P	Peer-to-peer client programs	These programs are used for managing peer-to-peer networks. Intruders can use them to spread malware programs.
Client-SMTP	SMTP clients	These programs send e-mail messages and hide this activity. Intruders install them on users' computers to send spam using users' idnetities.
WebToolbar	Web toolbars	These programs add their own search toolbars to other browsers' toolbars.
FraudTool	Fraud programs	These programs camouflage as other real programs. For example, fraudulent anti-virus programs display messages about detecting malware programs, but they do not find or disinfect anything.

METHODS OF DETECTING INFECTED, SUSPICIOUS AND POTENTIALLY DANGEROUS OBJECTS BY THE APPLICATION

Kaspersky Anti-Virus detects malware programs in objects using two methods: *reactive* (using databases) and *proactive* (using heuristic analysis).

The application's databases contain records that are used to identify any of the hundreds of thousands known threats in scanned objects. These records contain information both about the control sections of the malware programs' code, and algorithms for disinfecting the objects containing these programs. Kaspersky Lab's anti-virus analysts analyze hundreds of new malware programs on a daily basis, create records that identify them and include them in updates to the database files.

If, in a scanned object, Kaspersky Anti-Virus detects sections of code that fully match the control code sections of a malware program based on a database record, it sets the object's status to *infected*: if there is a partial match, the status is set to *suspicious*.

Using the proactive method, the application can detect new malicious programs which are not yet listed in the database.

The application detects objects containing new malware programs based on their behavior. The code of a new malware program may not fully or even partially coincide with that of a known malware program, but it will contain characteristic command sequences, such as opening a file, writing to a file, or intercepting interrupt vectors. The application can determine, for example, whether a file is infected with an unknown boot virus.

Objects detected using the proactive method are given the status *potentially dangerous*.

INSTALLING THE APPLICATION

The application is interactively installed on the computer, using the Application Setup wizard.

> Warning!
>
> We recommend that you close all running applications before proceeding with the installation.

To install the application on your computer run the distribution file, which has a .exe extension.

> Note
>
> Installing the application from the installation file downloaded via the Internet, is identical to installing the application from the CD.

The setup program is implemented as a standard Windows wizard. Each window contains a set of buttons to control the installation process. Provided below is the brief description of their purpose:

- **Next** – accept the action and move to the next step in the installation process.
- **Previous** – return to the previous step in the installation process.
- **Cancel** – cancel the installation.
- **Finish** – complete the application installation procedure.

A detailed discussion of each step of the package installation is provided below.

IN THIS SECTION:

Step 1. Searching for a newer version of the application 37

Step 2. Verifying the system satisfies the installation requirements 37

Step 3. Wizard's greeting window 38

Step 4. Viewing the License Agreement 39

Step 5. Selecting the installation type 39

Step 6. Selecting the installation folder 40

Step 7. Selecting application components to be installed 40

Step 8. Searching for other anti-virus software 41

Step 9. Final preparation for the installation 42

Step 10. Completing the installation 43

STEP 1. SEARCHING FOR A NEWER VERSION OF THE APPLICATION

Before installing the application on your computer, the wizard will access Kaspersky Lab's update servers to check whether a newer version exists.

If a newer version is not detected on Kaspersky Lab's update servers, the setup wizard will be started and install the current version.

If a newer version was detected on Kaspersky Lab’s update servers, you will be asked whether you want to download and install it. If you cancel the download, the setup wizard will start to install the current version. If you decide to install the newer version, the installation files will be downloaded to your computer, and the setup wizard will automatically start to install the newer version. For more details

on installing a newer version of the application, please refer to that version's documentation.

STEP 2. VERIFYING THE SYSTEM SATISFIES THE INSTALLATION REQUIREMENTS

Before installing the application on your computer, the wizard will verify that the computer satisfies the minimum requirements (see section "Hardware and Software System Requirements" on page 13). It will also verify that you have the rights required to install software on it.

If any of the requirements is not met, a corresponding notification will be displayed on the screen. We recommend that you install the required updates using the **Windows Update** service, and the required programs, before attempting to install Kaspersky Anti-Virus again.

STEP 3. WIZARD'S GREETING WINDOW

If your system meets the system requirements (see section "Hardware and Software System Requirements" on page 13), and either no newer version of the application was found on Kaspersky Lab's update servers or you cancelled installation of that version, the setup wizard will be started to install the current version of the application.

The setup wizard's first dialog box, indicating that it is about to start the installation, will be displayed on the screen.

To proceed with the installation press the **Next** button. To cancel installation, press the **Cancel** button.

STEP 4. VIEWING THE LICENSE AGREEMENT

The wizard's next dialog box contains the license agreement between you and Kaspersky Lab. Read it carefully, and if you agree with all terms and conditions of the agreement, select **I accept the terms of the license agreement** and press the **Next** button. The installation will be continued.

To cancel the installation, press the **Cancel** button.

STEP 5. SELECTING THE INSTALLATION TYPE

During this step you will be asked to select the installation type that suits you best:

- **Express installation**. If you select this option, the entire application will be installed on your computer with the default protection settings recommended by Kaspersky Lab. Once the installation is complete, the Application Configuration wizard will be started.

- **Custom installation**. In you select this option, you will be asked: to select which of the application's components you wish to install; to specify the folder into which the application will be installed (see section “Step 6. Selecting the Installation Folder” on page 40); to activate the application; and to configure it using the Application Configuration wizard.

If you select the first option, the application installation wizard will proceed directly to Step 8 *(*see section “Step 8. Searching for other anti-virus applications” on page 41). Otherwise your input or confirmation will be required at each step of the installation.

STEP 6. SELECTING THE INSTALLATION FOLDER

Note

This step of the installation wizard will be performed only if you selected the custom installation option (see section “Step 5. Selecting the installation type” on page 39).

During this step you will be asked to identify the folder on your computer into which the application will be installed. The default path is:

- **<Drive> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2009** – for 32-bit systems.

- **<Drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2009** – for 64-bit systems.

You can specify a different folder by pressing the **Browse** button and selecting a folder in the standard folder select dialog box, or by entering the folder’s path in the entry field provided.

Warning!

Please note that if you manually enter the full path to the installation folder, its length should not exceed 200 characters, and the path should not contain special characters.

To proceed with the installation press the **Next** button.

STEP 7. SELECTING APPLICATION COMPONENTS TO BE INSTALLED

Note. This step of the installation wizard will be performed only if you selected the custom installation option (see section “Step 5. Selecting the Installation Type” on page 39).

During a custom installation you must select which of the application's components you wish to be installed on your computer. By default, all the application's components are selected: protection, scanning and updating components.

To help you decide which components you wish to install, some information is available about each component: select the component from the list and read the information in the field below. The information includes a brief description of the component and the free hard drive space required for its installation.

To prevent the installation of any component, open the shortcut menu by clicking the icon next to the component's name, and select the **Component will not be available** item. Note that if you cancel installation of any component you will not be protected against a number of hazardous programs.

To select a component to be installed, open the shortcut menu by clicking the icon next to the component's name, and select **Component will be installed on local hard drive**.

When you have finished selecting components to be installed, press the **Next** button. To return to the default list of components to be installed, press the **Clear** button.

STEP 8. SEARCHING FOR OTHER ANTI-VIRUS SOFTWARE

During this step the wizard searches for other anti-virus programs, including other Kaspersky Lab programs, which may conflict with this application.

If any such programs were detected on your computer, they will be listed on the screen. You will be asked to uninstall them before you proceed with the installation.

You can choose whether to remove them automatically or manually, using the controls located below the list of detected anti-virus programs.

If the list of detected anti-virus programs includes Kaspersky Lab's 7.0 application, save that program’s key file when you uninstall it. You can use this key for the current version of the application. We also recommend that you save the objects stored in the quarantine and in the backup storage; these objects will

be automatically moved to the quarantine of the current version, and you will be able to re-scan them after the installation.

If you select automatic removal of the 7.0 version, information about its activation will be saved, and re-used during the installation of version 2009.

Warning!

The application accepts key files for versions 6.0 and 7.0. Keys used by version 5.0 and earlier are not supported.

To proceed with the installation press the **Next** button.

STEP 9. FINAL PREPARATION FOR THE INSTALLATION

This step completes the preparation for installing the application on your computer.

The first time you perform a custom application installation (see section "Step 5. Selecting the installation type" on page 39) we recommend that you do **not** uncheck the **Enable Self-Defense before installation** box. Enabling this option allows a correct installation rollback procedure, if an error occurs during the installation. When you retry the installation we recommend that you uncheck this box.

Note

If the application is being remotely installed using **Remote Desktop,** you are advised to uncheck the **Enable Self-Defense before installation** box. If this box is checked, the installation procedure may be performed incorrectly or not performed at all.

To proceed with the installation press the **Next** button. The installation files will start copying to your computer.

Warning!

During the installation process, the current network connection will be severed if the application package includes components for intercepting network traffic. The majority of terminated connections will be restored in due course.

STEP 10. COMPLETING THE INSTALLATION

The **Installation complete** window contains information on completing the installation of the application on your computer.

For instance, this window will indicate whether it is necessary to restart the computer to correctly complete the installation. After the system restart, the setup wizard will be automatically started.

If a system restart is not required, press the **Next** button to start the application configuration wizard.

APPLICATION INTERFACE

The application has a fairly simple and easy-to-use interface. This chapter discusses its basic features in detail.

In addition to the main application interface, there are plug-ins for Microsoft Outlook, The Bat! and Microsoft Windows Explorer. These plug-ins extend the functionality of these programs, as they allow Kaspersky Anti-Virus components to be managed and configured from the client program's interface.

IN THIS SECTION:

Notification area icon 44

Shortcut menu 45

Main application window 47

Notifications 50

Application settings window 50

NOTIFICATION AREA ICON

Immediately after installing the application, the application icon will appear in the Microsoft Windows taskbar notification area.

This icon indicates the application's current operation. It also reflects the protection status, and shows a number of basic functions performed by the program.

If the icon is active (color), all or some of the application's protection components are running. If the icon is inactive (black and white), all protection components have been disabled.

The application icon changes depending on the operation being performed:

– e-mail being scanned.

– updating application databases and program modules.

– computer needs to be rebooted to apply updates.

– an error has occurred in some Kaspersky Anti-Virus component.

The icon also provides access to the basics of the program interface, including the shortcut menu (see section "Shortcut menu" on page 45) and the main application window (see section "Main application window" on page 47).

To open the shortcut menu, right-click on the application icon.

To open the main application window, double click the application icon. The main window always opens at the **Protection** section.

If news from Kaspersky Lab is available, the news icon will appear in the taskbar notification area . Double click on the icon to view the news in the resulting window.

SHORTCUT MENU

You can run basic protection tasks from the context menu, which contains these items:

- **Update** – start the application module and database updates and install updates on your computer.
- **Full computer scan** – start a complete scan of the computer for dangerous objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Virus scan** – select objects and start a virus scan. The default list for this scan contains several objects, such as the **My documents** folder and e-mail archives. You can add to this list by selecting other objects to be scanned.

- **Kaspersky Anti-Virus** – open the main application window (see section "Main application window" on page 47).

- **Settings** – view and modify the application settings.

- **Activate** – activate the program. To become a registered user, you must activate your application. This menu item is only available if the application has not been activated.

- **About** – display information about the application.

- **Pause protection** / **Resume protection** – temporarily disable or enable the real-time protection components. This menu option does not affect the application's updates or virus scan task execution.

- **Exit** – close the application and unload the application from the computer's memory.

Figure 1: Shortcut menu

If a virus scan task is running when you open the shortcut menu, its name as well as its progress status (percentage complete) will be displayed in the shortcut menu. By selecting the task you will open the main application window which contains a report about the current results of the task's execution.

MAIN APPLICATION WINDOW

The main application window can be divided into three parts:

- The top part of the window indicates your computer's current protection status.

Figure 2: Current status of the computer protection

There are three possible values of protection status: each status is indicated by a certain color, similar to traffic lights. Green indicates that your computer's protection is at the correct level, while yellow and red colors indicate that there are security threats in the system configuration or in the application's operation. In addition to malware programs, threats include obsolete application databases, disabled protection components, and the selection of minimum protection settings.

Security threats must be eliminated as they appear. To obtain detailed information about them and to eliminate them quickly, use the **Fix it now** link (see figure above).

- The left-hand part of the window, the navigation bar, provides quick access to the application's functions, including anti-virus scans and updating tasks.

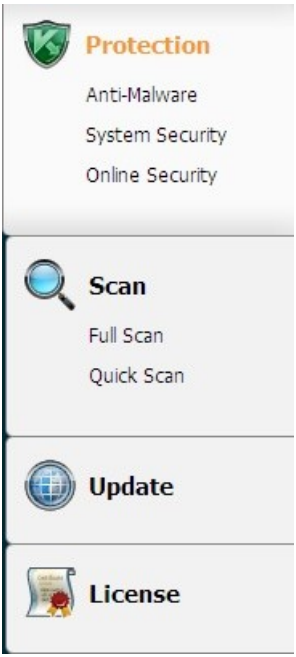

Figure 3: Left part of the main window

- The right-hand part of the window contains information about the application function selected in the left-hand part, and is used to configure those functions and display tools for performing anti-virus scan tasks, downloading updates, etc.

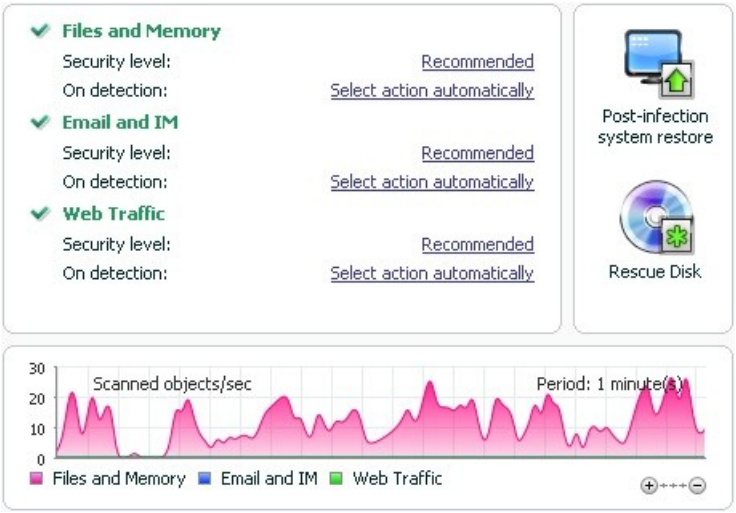

Figure 4: Informational part of the main window

You can also use these buttons:

- **Settings** – to open the application configuration window.
- **Help** – to open the application's Help system.
- **Detected** – to open the list of harmful objects detected by any component or scan task, and to view detailed statistics of the application's operation.
- **Reports** – to open the list of events which occurred during the application's operation.
- **Support** – to display information about the system, and links to Kaspersky Lab's information resources, including the Technical Support service site and the forum.

Note

You can change the appearance of the application by creating and using your own graphics and color schemes.

NOTIFICATIONS

If events occur during the application's operation, special notifications will be displayed on the screen as pop-up messages above the application's icon, in the Microsoft Windows task bar.

Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alert**. A critical event has occurred; for instance, a virus or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. This type of notification is in red.

- **Warning**! A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity has been detected on your system. You must instruct the program depending on how dangerous you think this event is. This type of notification is in yellow.

- **Note**: This notification gives information about non-critical events. This type, for example, includes notifications related to the operation of the **Content Filtering** component. Informational notifications are in green.

APPLICATION SETTINGS WINDOW

The application settings window can be opened from the main application window (see section "Main application window" on page 47) or the shortcut menu (see section "Shortcut menu" on page 45). To open the window, click the **Settings** link in the top part of the main application window, or select the appropriate option on the application shortcut menu.

The settings configuration window consists of two parts:

- the left-hand part of the window provides access to the application's components, such as virus scan tasks, and updating tasks;

- the right part of the window contains a list of settings for the component or task selected in the left part of the window.

GETTING STARTED

One of the main goals of Kaspersky Lab in making Kaspersky Anti-Virus was to provide the optimum configuration for all the application's options. This allows even an unsophisticated computer user to protect his or her computer immediately after installation, without spending hours changing the settings.

For the user's convenience, we have combined the preliminary configuration stages into a unified Initial Setup Wizard that starts as soon as the application is installed. By following the wizard's instructions, you can activate the application, configure settings for updates, restrict access to the program using a password, and perform other settings.

Your computer might be infected with malware before the application is installed. To detect existing malware programs, run a computer scan (see section “Anti-Virus computer scan” on page 54).

As the result of an infection by malware or system failures, your computer’s settings might be corrupted. Run the Security analysis wizard to find any vulnerabilities in installed software and anomalies in the system settings.

The application databases included in the installation package will probably be outdated. Start updating the application (see page 53), if it was not done by the configuration wizard, or automatically immediately after the application was installed.

After completing the actions in this section, the application will be ready to protect your computer. To evaluate your computer’s protection, use the Security Management wizard (see section “Security management” on page 60).

IN THIS SECTION:

Updating the application 53

Security analysis 54

Scanning computer for viruses 54

Managing license 55

Subscription for the automatic license renewal 56

Participating in the Kaspersky Security Network 59

Security management 60

Pausing protection 62

UPDATING THE APPLICATION

Warning!

You will need an internet connection to update Kaspersky Anti-Virus.

Databases containing threat signatures are included in the application distribution kit. However, when the application is installed the databases may already be obsolete, since Kaspersky Lab updates the databases and the application's modules on a regular basis.

You can specify how the updating task will launch when the application setup wizard runs. By default, Kaspersky Anti-Virus automatically checks for updates on Kaspersky Lab's update servers. If the server contains new updates, the application will silently download and install them.

To keep your computer's protection up to date, you are advised to update Kaspersky Anti-Virus immediately after installation.

- *To manually update Kaspersky Anti-Virus,*

    1. Open the main application window.

    2. Select the **Update** section in the left window side.

    3. Press the **Start update** button.

As a result, Kaspersky Anti-Virus will begin to be updated. The details of the process will be displayed in a special window.

SECURITY ANALYSIS

Your computer's operating system can be damaged by system failures and by the activities of malware programs. Additionally, user applications installed on your computer can have vulnerabilities which intruders can exploit to damage your computer.

To detect and eliminate such security problems, you are advised to launch the *Security Analyzer Wizard* immediately after you have installed the application. The security analysis wizard searches for vulnerabilities in installed applications, and for damage and anomalies in the operating system's and the browser's settings.

- *To start the wizard:*

    1. Open the main application window.

    2. In the left part of the window, select **System Security**.

    3. Start the **Security Analyzer** task.

SCANNING COMPUTER FOR VIRUSES

Developers of malware make every effort to conceal the actions of their programs, and therefore you may not notice the presence of malware programs in your computer.

Once Kaspersky Anti-Virus is installed on your computer, it automatically performs a **Quick scan** task on your computer. This task searches for and neutralizes harmful programs in the objects which are loaded when the operating system starts.

Kaspersky Lab's specialists also recommend that you perform the **Full scan** task.

- *To start / stop virus scan task:*

  1. Open the main application window.

  2. In the left-hand part of the window select the **Scan** (**Full scan**, **Quick scan**) section.

  3. Click the **Start scan** button to start the scan. If you need to stop the task, press the **Stop scan** button while the task is in progress.

MANAGING LICENSE

Kaspersky Anti-Virus needs a license key to operate. You will be provided with a key when you buy the program. It gives you the right to use the program from the day you purchase it and install the key.

Without a license key, unless a trial version of Kaspersky Anti-Virus has been activated, the application will run in the mode allowing only one update. The application will not download any new updates.

If a trial version of the program has been activated, after the trial period expires, Kaspersky Anti-Virus will not run.

When the license key expires, the program will continue working, except that you will not be able to update databases. As before, you will be able to scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your program license expires.

To protect your computer from infection with new viruses, we recommend that you renew your application key. Two weeks prior to the expiration of the application key the application will notify you about it. During some time a corresponding message will be displayed each time the application is launched.

Information on the current key is shown under **License** in the main window of Kaspersky Anti-Virus: key ID, type (commercial, commercial with subscription, commercial with protection subscription, trial, for beta testing), number of hosts on which this key may be installed, key expiration date and number of days remaining to expiration. Information about the key expiration will not be displayed if commercial license with subscription or commercial license with protection subscription is installed (see section "Subscription for the automatic license renewal" on page 56).

To view the provision of the application license agreement, click the **View End User License Agreement** button. To remove a key from the list, click the **Delete** button.

To purchase or renew a key:

1. Purchase a new key. To do it use the **Buy License** button (if the application was not activated) or **Renew license**. The resulting web page will contain all the information on purchasing a key through the Kaspersky Lab online store or corporate partners. If you purchase online, a key file or an activation code will be mailed to you at the address specified in the order form once payment has been made.

2. Install the key. To do it use the **Install key** button in the **License** section of the main application window or use command **Activation** from the main application menu. This will start the Activation Wizard.

Note. Kaspersky Lab regularly has special pricing offers on license extensions for our products. Check for specials on the Kaspersky Lab website in the **Products → Sales and special offers** area.

SUBSCRIPTION FOR THE AUTOMATIC LICENSE RENEWAL

When licensing using the subscription Kaspersky Anti-Virus will automatically contact the activation server in certain time intervals to maintain the validity of your license during the entire period of subscription.

If the current key has expired, Kaspersky Anti-Virus will check for the availability of an updated key at the server using background mode and if such key is found, the application will download it and install it in the previous key replacement

mode. This way the license will be renewed without your involvement. If the period during which the application renews the license itself has also expired, the license can be renewed manually. During the period allowing manual license renewal, the functionality of the application will be retained. After this period expires, if the license has not been renewed, it will no longer upload bases updates (for the commercial license with subscription), as well as will stop to ensure the protection of your computer (for the commercial license with protection subscription). To reject the subscription for automatic license renewal, contact our online store from which you have purchased the application.

Warning!

If by the moment of activation Kaspersky Anti-Virus is already activated using a commercial key, such commercial key will be replaced with a subscription key (a protection subscription key). If you wish to start using the commercial key again, you must delete the subscription key and activate the application again with the activation code using which you obtained the commercial key earlier.

The subscription condition is characterized by the following statuses:

1. *Corrupted*. Your request to activate the subscription has not yet been processed (some time is required for processing the request at the server). Kaspersky Anti-Virus operates in fully functional mode. If after a certain period of time the subscription request has not been processed, you will receive notification that the subscription has not been processed. In this case the application bases will not be updated any longer (for the commercial license with subscription), as well as the computer protection will not be performed (for the commercial license with protection subscription).

2. *Activation*. Subscription to automatic license renewal was activated for an unlimited period of time (no date specified) or for a certain time period (the subscription expiry date specified).

3. *Renewed*. Subscription was renewed automatically or manually for an unlimited period of time (no date specified) or for a certain time period (the subscription expiry date specified).

4. *Error*: Subscription renewal resulted in an error.

5. *Expired*. The subscription period has elapsed. You can use another activation code or renew your subscription by contacting online store you had purchased the application from.

6. *Subscription cancellation*. You cancel the subscription for the automatic license renewal.

7. *Update is required*. The key for subscription renewal has not been received on time for any reason. Use the **Renew subscription status** to renew the subscription.

For the commercial license with protection subscription, the subscription is characterized by two additional statuses:

- *Suspended*. The Subscription for the automatic license renewal suspended (subscription expiration date: subscription validity suspend date).

- *Resumed*. The Subscription for the automatic license renewal has been resumed (subscription expiration date is not limited).

If the subscription validity period has elapsed as well as the additional period during which license can be renewed (subscription status – *Expired*) Kaspersky Anti-Virus will notify you about it and will stop its attempts to obtain an updated key from the server. For the commercial license with subscription the functionality of the application will retain except the application bases update feature. For the commercial license with protection subscription the application bases will not be updated and the computer protection will not be performed.

If, for any reason, the license was not renewed (subscription status – *Update required*) in time (for example the computer was off during the entire time while the license renewal was available), you can renew its status manually. For this purpose you can use the **Renew subscription status** button. Until the moment of the subscription renewal Kaspersky Anti-Virus ceases to update the application databases (for the commercial license with subscription), as well as stops to perform the computer protection (for the commercial license with protection subscription).

While you are using the subscription you cannot install keys of other type or use another activation code to renew the license. You can use another activation code only after the subscription period is over (the subscription status – *Expired*).

Warning!

Note that when you use subscription for the automatic license renewal, if you reinstall the application on your computer, you will need to activate the product again manually using the activation code you obtained when you purchased the application.

PARTICIPATING IN THE KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on an everyday basis. To facilitate the gathering of statistics about new threat types, where they come from and how to eliminate them, Kaspersky Lab invites you to use the Kaspersky Security Network service.

The use of Kaspersky Security Network involves sending the following information to Kaspersky Lab:

- A unique identifier assigned to your computer by the application. This identifier characterizes the hardware settings of your computer, and does not contain any other information.
- Information about threats detected by the application. The structure and contents of the information depend on the type of threat detected.
- System information: the operating system version, installed service packs, downloadable services and drivers, browser and e-mail client program versions, browser extensions, version number of Kaspersky Anti-Virus installed.

Kaspersky Security Network also gathers extended statistics, including information about:

- executable files and signed applications downloaded on your computer;
- applications running on your computer.

This statistical information is sent once application updating is complete.

Warning!

Kaspersky Lab guarantees that no gathering or distribution of users' personal data is performed within Kaspersky Security Network.

▸ *To configure the sending of statistics:*

1. Open the application setting window.

2. Select the **Feedback** section in the left part of the window.

3. Check the box **I agree to participate in Kaspersky Security Network**, to confirm your participation in the Kaspersky Security Network. Check the box **I agree to send extended statistics within the framework of Kaspersky Security Network**, to confirm your consent to send extended statistics.

SECURITY MANAGEMENT

Problems in computer protection are indicated in the main application window by a change of the color of the protection status icon and of the panel in which this icon is located. Once problems appear in the protection system, you are advised to deal with them immediately.

Figure 5: Current status of the computer protection

You can view the list of current problems, their description and possible solutions on the **Status** tab (see figure below) that opens when you click on the **Fix it now** link (see figure above).

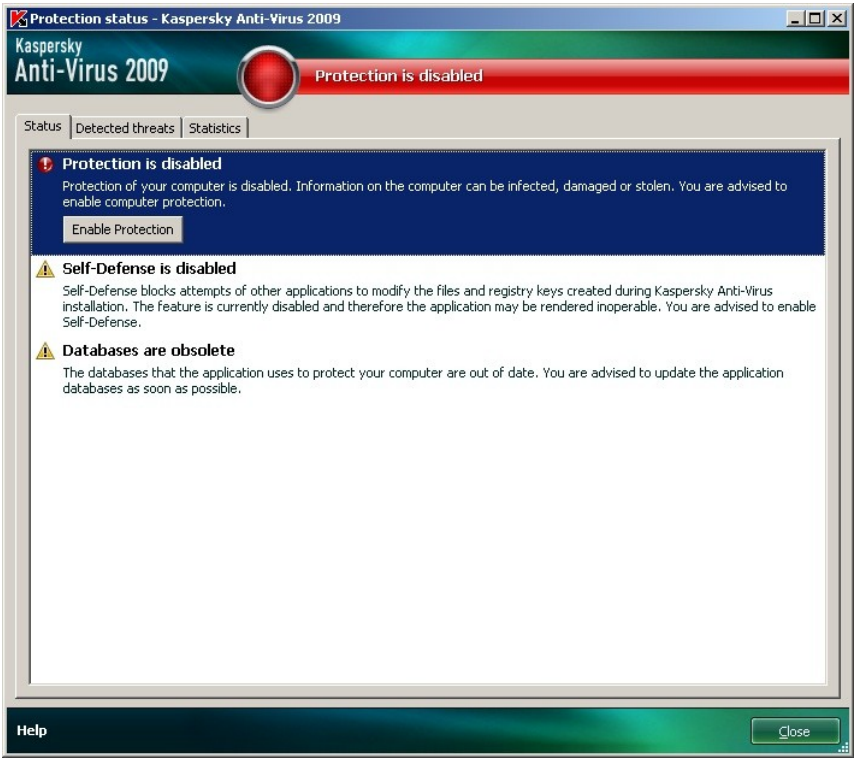
Protection status - Kaspersky Anti-Virus 2009
Kaspersky
Anti-Virus 2009
Protection is disabled
Status
Detected threats
Statistics
Protection is disabled
Protection of your computer is disabled. Information on the computer can be infected, damaged or stolen. You are advised to enable computer protection.
Enable Protection
Self-Defense is disabled
Self-Defense blocks attempts of other applications to modify the files and registry keys created during Kaspersky Anti-Virus installation. The feature is currently disabled and therefore the application may be rendered inoperable. You are advised to enable Self-Defense.
Databases are obsolete
The databases that the application uses to protect your computer are out of date. You are advised to update the application databases as soon as possible.
Help
Close

Figure 6: Solving security problems

The tab shows the list of current problems. Problems are listed in order of importance: first, the most critical problems, marked with the red status icon; second, less important problems, marked by the yellow status icon, and finally information messages, marked by a green icon. A detailed description is provided for each problem, and the following actions are available:

- *Eliminate immediately*. Using the corresponding buttons, you can start to fix the problem, which is the recommended action.

- *Postpone elimination*. If, for any reason, you cannot immediately eliminate the problem, you can delay this action and return to it later. To postpone elimination, use the **Hide message** button.

  Note that this option is not available for serious problems. Such problems include, for example, malicious objects which were detected but not disinfected, crashes of one or several components, or corruption of the application files.

To make hidden messages re-appear in the general list, check the **Show hidden messages** box.

PAUSING PROTECTION

Pausing protection means temporarily disabling all protection components for a certain period of time.

- *To pause the protection of your computer:*

  1. Select the **Pausing protection** item from the application's shortcut menu (see section "Shortcut menu" on page 45).

  2. In the window that opens, select the period of time for which you want protection to be paused:

     - **In <time interval>** – protection will be enabled after this length of time elapses. Use the dropdown menu to select the time interval value.

     - **After restart** – protection will be enabled after the system restarts, provided that the application is also configured to launch when the computer reboots.

     - **Manually** – protection will resume only after you start it manually. To enable protection, select **Resume protection** from the application's shortcut menu.

As a result of temporarily disabling protection, all protection components will be paused. This is indicated by:

- Inactive (grey) names of disabled components in the **Protection** section of the main window.
- Inactive (grey) application icon (see section “Notification area icon” on page 44) in the system panel.
- Red color for the status icon and for the main application window's panel.

If new network connections were being established at the same time as protection was paused, a notification will be displayed about disruptions to those connections.

VALIDATING APPLICATION SETTINGS

After the application has been installed and configured, you should verify whether the application is correctly configured using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION:

Test the EICAR "virus" and its modifications 64

Testing the HTTP traffic protection 68

Testing the SMTP traffic protection 68

Validating File Anti-Virus settings 69

Validating virus scan task settings 70

TEST THE EICAR "VIRUS" AND ITS MODIFICATIONS

This test "virus" was specially designed by eicar (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test "virus" IS NOT A VIRUS, because it does not contain code that can harm your computer. However, most manufacturers of anti-virus products identify this file as a virus.

> Warning!
>
> Never use real viruses to test the operation of an anti-virus product!

You can download the test “virus” from the **EICAR** organization’s official website at: http://www.eicar.org/anti_virus_test_file.htm.

Note

Before you download the file, you must disable the computer’s anti-virus protection, because otherwise the application would identify and process the file *anti_virus_test_file.htm* as an infected object transferred via HTTP protocol.

Do not forget to enable the anti-virus protection immediately after you download the test “virus”.

The application identifies the files downloaded from the **EICAR** site as an infected object containing a virus that **cannot be disinfected** and performs the actions specified for such an object.

You can also modify the standard test “virus” to verify the application’s operation against other types of files. To modify the “virus”, change the content of the standard “virus” by adding one of the prefixes to it (see table below). To create the modified “virus” files, you can use any text or hypertext editor, for example **Microsoft Notepad**, **UltraEdit32**, etc.

Warning!

You can test the correctness of the application’s operation using the modified EICAR “virus” only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

In the table below, the first column contains the prefixes that must be added at the start of the standard “virus” text. The second column lists the possible status values that the application can assign to the object, based on the results of the scan. The third column indicates how the application processes objects with the specified status. Please note that the actual actions performed on the objects are determined by the application's settings.

After you have added the prefix to the test “virus”, save the new file under a different name, for example: *eicar_dele.com*. Assign similar names to all the modified “viruses”.

Table 6. Modifications of the test "virus"

Prefix	Object status	Object processing information
No prefix, standard test virus	**Infected**. Infected object contains code of a known virus. Disinfection is not possible.	The application identifies the object as a non-disinfectible virus. An error occurs while attempting to disinfect the object; the action assigned to be performed with non-disinfectible objects will be applied.
CORR–	**Corrupted**.	The application could access the object, but was unable to scan it because the object is corrupted (for example, the file structure is corrupted or file format is invalid). Information about how the object was processed can be found in the application operation report.
WARN–	**Suspicious**. Object contains code of an unknown virus. Disinfection is not possible.	The object has been found suspicious by the heuristic code analyzer. At the time of detection, the application's databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
SUSP–	**Suspicious**. Object contains modified code of a known virus. Disinfection is not possible.	The application detected a partial correspondence of a section of the object's code with a section of code of a known virus. At the time of detection, the application's databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.

Prefix	Object status	Object processing information
ERRO–	Scanning error	An error occurred while scanning the object. The application was unable to access the object: either the object's integrity was breached (for example, no end to a multi-volume archive) or there is no connection to it (if the object being scanned is located on a network drive). You can find information about the object's processing in the application operation's report.
CURE–	**Infected**. Object contains code of a known virus. Disinfectible.	The object contains a virus that can be disinfected. The application will disinfect the object; the text of the "virus" body will be replaced with the word CURE. You will be notified when an object of this type is detected.
DELE–	**Infected**. Object contains code of a known virus. Disinfection is not possible.	The application identifies the object as a non-disinfectible virus. An error occurs at the attempt to disinfect the object; the action performed will be that specified for non-disinfectible objects. You will be notified when an object of this type is detected.

TESTING THE HTTP TRAFFIC PROTECTION

- *In order to verify that viruses are successfully detected in data streams transferred via the HTTP protocol, do the following:*

  try to download a test "virus" from the official website of the **EICAR** organization at: http://www.eicar.org/anti_virus_test_file.htm.

When attempting to download the test "virus", Kaspersky Anti-Virus will detect this object, identify it as an infected object that cannot be disinfected, and will perform the action specified in the HTTP traffic settings for objects with this status. By default, when you attempt to download the test "virus", the connection with the website will be terminated and the browser will display a message informing the user that this object is infected with the EICAR-Test-File virus.

TESTING THE SMTP TRAFFIC PROTECTION

To detect viruses in data streams transferred using the SMTP protocol, you must transfer data using an e-mail system that uses this protocol.

Note

We recommend that you test how Kaspersky Anti-Virus handles incoming **and** outgoing e-mail messages, including both the body of the message and the attachments. To test the detection of viruses in message bodies, copy the text of the standard test "virus", or of the modified "virus", into the body of the message.

- *To test virus detection in SMTP data streams:*

  1. Create a **Plain text** format message using an e-mail client installed on your computer.

> Note
>
> A message that contains a test virus will not be scanned if it is created in RTF or HTML format!

2. Copy the text of the standard or modified “virus” at the beginning of the message, or attach a file containing the test “virus” to the message.

3. Send the message to the administrator.

The application will detect the object, identify it as infected, and block the message.

VALIDATING FILE ANTI-VIRUS SETTINGS

- *To verify that the File Anti-Virus component is correctly configured:*

  1. Create a folder on a disk, and copy into the folder the EICAR test “virus” which you downloaded, and the modified test “viruses” which you created.

  2. Check that all events will be logged, so that the report file will retain data on both corrupted objects, and on objects not scanned because of errors.

  3. Run the test “virus” or one of its modified versions.

The File Anti-Virus will intercept the call to the file, scan it, and will perform the action specified in the settings for objects of that status. By selecting different actions to be performed on the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

- *To verify that the anti-virus scan task is correctly configured:*

  1. Create a folder on a disk, and copy into the folder the EICAR test “virus” which you downloaded, and the modified test “viruses” which you created.

  2. Create a new virus scan task and select the folder which contains the set of test “viruses”, as the object to scan.

  3. Check that all events are logged, so that the report file will retain data about corrupted objects, and about objects not scanned because of errors.

  4. Run the virus scan task.

When the scan task is running, the actions specified in the task configuration will be performed as suspicious or infected objects are detected. By selecting various actions to be performed on detected objects, you will be able to fully check the component's operation.

You can view detailed information about the task’s actions in the report on the component's operation.

KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

INTRODUCTION

PLEASE READ THIS DOCUMENT CAREFULLY. IT CONTAINS IMPORTANT INFORMATION THAT YOU SHOULD KNOW BEFORE CONTINUING TO USE OUR SERVICES OR SOFTWARE. BY CONTINUING TO USE KASPERSKY LAB SOFTWARE AND SERVICES YOU WILL BE DEEMED TO HAVE ACCEPTED THIS KASPERSKY LAB' Data Collection STATEMENT. We reserve the right to modify this Data Collection Statement at any time by posting the changes on this page. Please check the revision date below to determine if the policy has been modified since you last reviewed it. Your continued use of any portion of Kaspersky Lab's Services following posting of the updated Data Collection Statement shall constitute your acceptance of the changes.

Kaspersky Lab and its affiliates (collectively, "***Kaspersky Lab"***) has created this Data Collection Statement in order to inform and disclose its data gathering and dissemination practices for Kaspersky Anti-Virus and Kaspersky Internet Security.

Word from Kaspersky Lab

Kaspersky Lab has a strong commitment to providing superior service to all of our customers and particularly respecting your concerns about Data Collection. We understand that you may have questions about how Kaspersky Security Network collects and uses information and data and we have prepared this statement to inform you of the Data Collection principles that govern the Kaspersky Security Network (the "***Data Collection Statement"*** or "***Statement"***).

This Data Collection Statement contains numerous general and technical details about the steps we take to respect your Data Collection concerns. We have organized this Data Collection Statement by major processes and areas so that you can quickly review the information of most interest to you. The bottom line is that meeting your needs and expectations forms the foundation of everything we do - including protecting your Data Collection.

The data and information is collected by Kaspersky Lab and if after reviewing this Data Collection Statement you have any questions or Data Collection concerns please send an e-mail to support@kaspersky.com.

What is Kaspersky Security Network?

Kaspersky Security Network service allows users of Kaspersky Lab security products from around the world to help facilitate identification and reduce the time it takes to provide protection against new ("in the wild") security risks targeting your computer. In order to identify new threats and their sources and to help improve user security and product functionality, Kaspersky Security Network collects selected security and application data about potential security risks targeting your computer and submits that data to Kaspersky Lab for analysis. **Such information contains no personally identifiable information about the user and is utilized by Kaspersky Lab for no other purposes but to enhance its security products and to further advance solutions against malicious threats and viruses. In case of accidental transmission of any personal data of the user, Kaspersky Lab shall keep and protect it in accordance with this Data Collection Statement**.

By participating in Kaspersky Security Network, you and the other users of Kaspersky Lab security products from around the world contribute significantly to a safer Internet environment.

Legal Issues

Kaspersky Security Network may be subject to the laws of several jurisdictions because its services may be used in different jurisdictions, including the United States of America. Kaspersky Lab shall disclose personally identifiable information without your permission when required by law, or in good-faith belief that such action is necessary to investigate or protect against harmful activities to Kaspersky Lab guests, visitors, associates, or property or to others. As mentioned above, laws related to data and information collected by Kaspersky Security Network may vary by country. For example, some personally identifiable information collected in the European Union and its Member States is subject to the EU Directives concerning personal data, Privacy and electronic communications, including but not limited to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of Privacy in the electronic communications sector and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the subsequent legislation adopted in the EU Member States, the European Commission Decision 497/2001/EC on standard contractual clauses (personal

data transferred to third countries) and the subsequent legislation adopted in the EC Member States.

Kaspersky Security Network shall duly inform the users concerned, when initially collecting the above-mentioned information, of any sharing of such information, notably for use for business development and shall allow these Internet users to **opt in** (in the EC Member States and other countries requiring opt-in procedure) or opt-out (for all the other countries) on-line from the commercial use of this data and/or the transmission of this data to third parties.

Kaspersky Lab may be required by law enforcement or judicial authorities to provide some personally identifiable information to appropriate governmental authorities. If requested by law enforcement or judicial authorities, we shall provide this information upon receipt of the appropriate documentation. Kaspersky Lab may also provide information to law enforcement to protect its property and the health and safety of individuals as permitted by statute.

Declarations to Personal Data Protection Member States authorities shall be made according to the subsequent EU Member States legislation in force. Information about such declarations shall be accessible on the Kaspersky Security Network services.

COLLECTED INFORMATION

Data We Collect

The Kaspersky Security Network service will collect and submit core and extended data to Kaspersky Lab about potential security risks targeting your computer. The data collected includes:

Core data

- information about your computer hardware and software, including operating system and service packs installed, kernel objects, drivers, services, Internet Explorer extensions, printing extensions, Windows Explorer extensions, downloaded program files, active setup elements, control panel applets, host and registry records, IP addresses, browser types, e-mail clients and the version number of the Kaspersky Lab product, that is generally not personally identifiable;

- a unique ID that is generated by the Kaspersky Lab product to identify individual machines without identifying the user and which does not contain any personal information;

- information about the status of your computer's antivirus protection, and data on any files or activities suspected of being malware (e.g., virus name, date/time of detection, names/paths and size of infected files, IP and port of network attack, name of the application suspected of being malware). Please note that the above referenced collected data does not contain personally identifiable information.

Extended data

- Information about digitally signed applications downloaded by the user (URL, file size, signer name)

- Information about executable applications (size, attributes, date created, information about PE headers, region, name, location, and compression utility used).

Securing the Transmission and Storage of Data

Kaspersky Lab is committed to protecting the security of the information it collects. The information collected is stored on computer servers with limited and controlled access. Kaspersky Lab operates secure data networks protected by industry standard firewall and password protection systems. Kaspersky Lab uses a wide range of security technologies and procedures to protect the information collected from threats such as unauthorized access, use, or disclosure. Our security policies are periodically reviewed and enhanced as necessary, and only authorized individuals have access to the data that we collect. Kaspersky Lab takes steps to ensure that your information is treated securely and in accordance with this Statement. Unfortunately, no data transmission can be guaranteed secure. As a result, while we strive to protect your data, we cannot guarantee the security of any data you transmit to us or from our products or services, including without limitation Kaspersky Security Network, and you use all these services at your own risk.

The data that is collected may be transferred to Kaspersky Lab servers and Kaspersky Lab has taken the necessary precautions to ensure that the collected information, if transferred, receives an appropriate level of protection We treat the data we collect as confidential information; it is, accordingly, subject to our security procedures and corporate policies regarding protection and use of confidential information. After collected data reaches Kaspersky Lab it is stored on a server with physical and electronic security features as customary in the industry, including utilization of login/password procedures and electronic firewalls designed to block unauthorized access from outside of Kaspersky Lab. Data collected by Kaspersky Security Network covered by this Statement is

processed and stored in the United States and possibly other jurisdictions and also in other countries where Kaspersky Lab conduct business. All Kaspersky Lab employees are aware of our security policies. Your data is only accessible to those employees who need it in order to perform their jobs. Any stored data will not be associated with any personally identifiable information. Kaspersky Lab does not combine the data stored by Kaspersky Security Network with any data, contact lists, or subscription information that is collected by Kaspersky Lab for promotional or other purposes.

USE OF THE COLLECTED DATA

How Your Personal Information Is Used

Kaspersky Lab collects the data in order to analyze and identify the source of potential security risks, and to improve the ability of Kaspersky Lab's products to detect malicious behavior, fraudulent websites, crimeware, and other types of Internet security threats to provide the best possible level of protection to Kaspersky Lab customers in the future.

Disclosure of Information to Third Parties

Kaspersky Lab may disclose any of the information collected if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process or if we believe in good faith that we are required to do so in order to comply with applicable law, regulation a subpoena, or other legal process or enforceable government request. Kaspersky Lab may also disclose personally identifiable information when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating this Statement, the terms of your agreements with the Company or to protect the safety of our users and the public or under confidentiality and licensing agreements with certain third parties which assist us in developing, operating and maintaining the Kaspersky Security Network. In order to promote awareness, detection and prevention of Internet security risks, Kaspersky Lab may share certain information with research organizations and other security software vendors. Kaspersky Lab may also make use of statistics derived from the information collected to track and publish reports on security risk trends.

Choices available to you

Participation in Kaspersky Security Network is optional. You can activate and deactivate the Kaspersky Security Network service at any time by visiting the Feedback settings under your Kaspersky Lab product's options page. Please

note, however, if you should choose to withhold requested information or data, we may not be able to provide you with some of the services dependent upon the collection of this data.

Once the service period of your Kaspersky Lab product ends, some of the functions of the Kaspersky Lab software may continue to operate, but information will no longer be sent automatically to Kaspersky Lab.

We also reserve the right to send infrequent alert messages to users to inform them of specific changes that may impact their ability to use our services that they have previously signed up for. We also reserve the right to contact you if compelled to do so as part of a legal proceeding or if there has been a violation of any applicable licensing, warranty and purchase agreements.

Kaspersky Lab is retaining these rights because in limited cases we feel that we may need the right to contact you as a matter of law or regarding matters that may be important to you. These rights do not allow us to contact you to market new or existing services if you have asked us not to do so, and issuance of these types of communications is rare.

DATA COLLECTION – RELATED INQUIRIES AND COMPLAINTS

Kaspersky Lab takes and addresses its users' Data Collection concerns with utmost respect and attention. If you believe that there was an instance of non-compliance with this Statement with regard to your information or data you have other related inquiries or concerns, you may write or contact Kaspersky Lab at email: support@kaspersky.com.

In your message, please describe in as much detail as possible the nature of your inquiry. We will investigate your inquiry or complaint promptly.

Provision of information is voluntary. An option of data collection can be disabled by the user at any time in section "**Feedback"** on the page "**Settings"** of any appropriate Kaspersky product.

Copyright © 2008 Kaspersky Lab. All rights reserved.

KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of high-performance data security software including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today Kaspersky Lab employs over 450 highly qualified specialists including 10 MBA degree holders and 16 PhD degree holders. Several of Kaspersky Lab’s senior experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company’s most valuable assets are the unique knowledge and expertise accumulated by its specialists during fourteen years fighting continuously against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee trends in malware development, and deliver to our users timely protection against new types of attacks. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain one step ahead of other vendors in delivering anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was one of the first businesses of its kind to develop many modern anti-virus software standards. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network: workstations, file servers, mail systems, firewalls, internet gateways and hand-held computers. Its convenient and easy-to-use management tools maximize the degree of automation of anti-virus protection for computers and corporate networks. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybaris (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers receive a wide range of additional services that ensure both stable operation of the company's products, and compliance with the

customer's specific business requirements. We design, implement and support corporate anti-virus complexes. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service available in several languages.

If you have any questions, you can contact our dealers or contact Kaspersky Lab directly. Detailed consultations are provided by phone or e-mail. You will receive full and comprehensive answers to any question.

Address:	Russia, 123060, Moscow, 1-st Volokolamsky Proezd, 10, Building 1
Tel., Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
24/7 Emergency Support:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Support of business product users:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (from 10 am until 7 pm) http://support.kaspersky.com/helpdesk.html
Support for corporate users:	Contact information will be provided after you purchase a corporate software product depending on your support package.
Kaspersky Lab web forum:	http://forum.kaspersky.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending new viruses in archives)
User documentation development group:	docfeedback@kaspersky.com (only for sending feedback on documentation and Help system)

Sales Department:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
General Information:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.com/ http://www.viruslist.com

CRYPTOEX LLC

To create and verify digital signatures, Kaspersky Anti-Virus uses Crypto Ex LLC's data security software library, Crypto C.

Crypto Ex holds a license from the Federal Agency for Government Communications and Information (a branch of the Federal Security Service) to develop, manufacture and distribute encryption software to protect data which does not constitute a state secret.

The Crypto C library is designed to protect KS1 class confidential information, and has been granted FSB compliance certificate No. SF/114-0901 dated July 1, 2006.

The library encrypts and decrypts fixed size data packs and/or data flows, using the following technologies:

- a cryptographic algorithm (GOST 28147-89);
- algorithms for generating and verifying electronic digital signature based on algorithms (GOST R 34.10-94 and GOST 34.10-2001);
- hash functions (GOST 34.11-94);
- generation of key information using a pseudorandom number program transmitter;
- a key information and simulation vector generation system (GOST 28147-89).

The library's modules were implemented in ANSI standard C, and can be integrated into applications either as statically and dynamically loaded code. It can be executed on a variety of platforms including x86, x86-64, Ultra SPARC II, and compatible platforms.

The library's modules can be migrated to the following operating environments: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris for Ultra SPARC II).

For more information, visit the CryptoEx LLC corporate website at http://www.cryptoex.ru, or contact the company by e-mail at info@cryptoex.ru.

MOZILLA FOUNDATION

The **Gecko SDK ver. 1.8** library was used for the development of this application's components.

This software is used according to the terms and conditions of license MPL 1.1 Public Mozilla Foundation license http://www.mozilla.org/MPL.

For more details about the **Gecko SDK** library, refer to:
http://developer.mozilla.org/en/docs/Gecko_SDK.

© Mozilla Foundation

Mozilla Foundation website: http://www.mozilla.org.

LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS AND PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER'S INTERNET WEB SITE, THE CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF THE PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR THE EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER CAN BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to “Software” herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as a part of the Kaspersky Anti-Virus.

1. *License Grant*. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use the Software and the accompanying documentation (the “Documentation”) for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer.

1.1 *Use*. If the Software was purchased on a physical medium you have the right to use the Software for protection of such a number of computers as indicated on the box. If the Software was purchased via Internet you have the right to use the Software for protection of such a number of computers as you ordered when purchased the Software.

1.1.1 The Software is “in use” on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software’s proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab's update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not provide the activation code or license key file to third parties or allow third parties access to the activation code or license key. The activation code and license key are confidential data.

1.1.8 Kaspersky Lab may ask you to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.10 Kaspersky Lab, with your consent explicitly confirmed in corresponding Statement, has the right to gather information about potential threats and vulnerabilities from your computer. The information thus gathered is used in a generic form for the sole purpose of improving Kaspersky Lab's products.

2. *Support* [1].

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period specified in the License Key File (service period) and indicated in the "Service" window, from the moment of activation on:

(a) payment of its then current support charge, and:

(b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to enter activation code also provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not

[1] When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).

you have satisfied this condition for the provision of Support Services.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from you additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) "Support Services" means:

(a) Regular updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates in 24-hours period.

(iv) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights*. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality*. You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement

reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the activation code.

5. *Limited Warranty*.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at in paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in paragraph (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability*.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i) above, the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.